

Notice of Allowability**Application No.**

10/773,717

Examiner

SHIN-HON CHEN

Applicant(s)

TOUTONGHI, MICHAEL J.

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to RCE filed on 4/14/08.
2. ☒ The allowed claim(s) is/are 1,4,5,7-9,13,15,18,19,21 and 22.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
(a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
(b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413),
Paper No./Mail Date 20080514.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. Claims 1, 4-9, 13, 15, and 18-22 have been examined.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 4/14/08 has been entered.

EXAMINER'S AMENDMENT

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Benjamin Tabor on 5/14/08.

The application has been amended as follows:

1. (Currently Amended) A method performed by a client comprising:
storing a secret in a secure storage;

receiving a password challenge from a server; and
responsive to the password challenge, calling a secure password prompt routine to
execute a procedure, wherein the procedure comprises:

- (1) accessing the secret in the secure storage;
- (2) generating an authentication graphic based on the secret; and
- (3) rendering a prompt at a display device, the prompt including a request

for user to input a password and the authentication graphic, which are visible to
the user; wherein the secure password prompt routine renders the authentication
graphic for all password challenges;

receiving the password from the user;

generating a digest with a cryptographically-safe function that includes indicia of
the received password and the received password challenge, wherein the digest is a
communication that securely protects the password from being intercepted; and

sending the digest to the server, wherein the server verifies the digest by
comparing it to a recalculated digest that includes an indicia of the password challenge
and a stored authentic password.

4. (Cancelled)

15. (Currently Amended) A machine-readable storage medium having stored thereon
data representing instructions that, when executed by a processor of a client, cause the processor
to perform operations comprising:

receiving a password challenge from a server;

responsive to the password challenge, calling, a secure password prompt routine to execute a procedure, wherein the procedure comprises:

- (1) accessing the secret in the secure storage;
- (2) generating an authentication graphic based on the secret; and
- (3) rendering a prompt at a display device, the prompt including a request for a user to input a password and the authentication graphic, which are visible to the user; wherein the secure password prompt routine renders the authentication graphic for all password challenges;

receiving the password from the user;

altering the received password utilizing a hash function;

generating a digest using the altered password and the received password challenge; and

sending the digest to the server without directly passing the password over a communications medium, wherein the server verifies the digest by comparing it to a recalculated digest that includes an indicia of the password challenge and a stored authentic password.

18. (Currently Amended) The ~~method~~ storage medium of claim 15, further comprising making the authentication graphic known to the user so that the user can identify the authentication graphic on the prompt prior to the user inputting a password in response to the prompt.

19. (Currently Amended) The ~~method~~ storage medium of claim 15, wherein making the authentication graphic known comprises physically attaching the authentication graphic to the client.

20. (Cancelled)

Allowable Subject Matter

4. The following is an examiner's statement of reasons for allowance: The closest prior art of record discloses a method for generating a password prompt that allows user to visually or audibly determine whether the password prompt is legitimate. However, the prior art of record individually or in combination does not explicitly disclose generating a digest that includes indicia of the received password and the received password challenge to protect the password from being intercepted in light of other features disclosed in independent claims 1, 9 and 15.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHIN-HON CHEN whose telephone number is (571)272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2131

Shin-Hon Chen
Examiner
Art Unit 2131

SC